# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

| AIR FORCE EQUAL OPPORTUNITY NETWORK (AFEON) |
| --- |
| DEPARTMENT OF THE AIR FORCE |

## SECTION 1: IS A PIA REQUIRED?

**a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).**

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

**b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.**

**c. If "Yes," then a PIA is required. Proceed to Section 2.**

## SECTION 2: PIA SUMMARY INFORMATION

**a. Why is this PIA being created or updated? Choose one:**

☒ **New DoD Information System** ☐ **New Electronic Collection**

☐ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

**b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?**

☒ **Yes, DITPR** Enter DITPR System Identification Number 1018829

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☐ **No**

**c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?**

☒ **Yes** ☐ **No**

**If "Yes," enter UPI** 007-57-06-20-01-????-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

**d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?**

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

**If "Yes," enter Privacy Act SORN Identifier** F036 AF DP G

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

**or**

**Date of submission for approval to Defense Privacy Office**
Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an OMB Control Number?**
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

**Enter OMB Control Number**

**Enter Expiration Date**

☒ **No**

**f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

Authority:
10 U.S.C. 8013, Secretary of the Air Force; Pub. L. 105-85, section 591; AFPD 36-27, Social Actions; Air Force Instruction 36-2706, Military Equal Opportunity and Treatment Program; For Sexual Assault: Pub L. 108-375, as amended and supplemented, October 28, 2004, Section 577(e); AFPD 36-60, Sexual Assault Prevention and Response (SAPR) Program and E.O. 9397 (SSN).
Purpose(s):
To investigate and resolve complaints of unlawful discrimination and sexual harassment under the Equal Opportunity Program, and to maintain records created as a result of the filing of allegations and appeals involving unlawful discrimination because of race, color, religion, sex, or national origin. To assist and provide victim services to victims of sexual assault under the Sexual Assault Prevention and Response Program, and to maintain records created as a result of restricted or unrestricted reporting of allegations of sexual assault under the Sexual Assault Prevention and Response Program.
To conduct necessary background checks of Sexual Assault Prevention and Response Program volunteers/personnel.
To report information as required by the FY 98 National Defense Authorization Act, and used as a data source for descriptive statistics.

**g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

AFEON is a system that consolidates all military and civilian Air Force Equal Opportunity Program operational and information technology services (data collection/case management & Climate Assessment Processing) through a single portal (similar to the AF Portal concept). The system is web-based and allows data-entry, data-management, and data-retrieval to support installation level EO offices, Major Command (MAJCOM) EO Strategic Advisors, HQ USAF/A1Q (Air Staff), AFPC/EO (EO Operations) Air Force Reserve, the Air National Guard EO programs and Secretary of the Air Force Civilian Appellate Review Office (SAF/MRB). Approximately 1,500 EO accounts at 485 locations is required. AFEON has one single point of entry into the IT system (one screen, one login) for both military and civilian users.
- AFEON allows for event driven data-entry of civilian pre, formal, and class complaints, military informal & formal complaints, unit climate assessment surveys data tabulation, EO incident reporting, and transferring of complaint data to other MAJCOMs and Installations.
- AFEON provides a Common Access Card (CAC) (.mil) web-based system for EO staff to securely document and upload case management data.
- AFEON is automatically upgraded by the vendor with the latest software patches and necessary upgrades and enhancements to keep the system up to date with the latest functionality, and EEOC guidance, laws, procedures, and reporting requirements.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Unless the system is hacked, vulnerability of privacy information is minimal. If the system is compromised, general customer demographic and a limited number of SSN accounts with associated date of birth information would be vulnerable.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)?** Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Air Force use

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. EEOC

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

**i. Do individuals have the opportunity to object to the collection of their PII?**

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

All personal data collected are voluntarily given by the subject individual. Forms that collect personal data to be maintained in this IT investment contain a Privacy Act Statement, as required by 5 USC. 552a(e), and in accordance with guidelines established in AFI 33-332, Privacy Act Program, Chapters 3 and 7, and 12, allowing the individual to make an informed decision about providing the data. The statement of understanding advises the individual that the information provided is voluntary and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the Air Force Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection.

(2) If "No," state the reason why individuals cannot object.

**j. Do individuals have the opportunity to consent to the specific uses of their PII?**

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Forms that collect personal data will contain a Privacy Act Statement, as required by 5 USC 552a(e)(3), and under Executive Order or EO 9397 and 13478 (SSN), as the authority to collect the social security number and in accordance with guidelines established in AFI 33-332, Privacy Act Program, Chapters 3 and 7, and 12, allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the Air Force Privacy Act Office during the comment period (if applicable), during data collection, or at any time after the program is launched. If no objections are received, consent is presumed.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

**k. What information is provided to an individual when asked to provide PII data?** Indicate all that apply.

| | | | |
|---|---|---|---|
| ☒ | **Privacy Act Statement** | ☐ | **Privacy Advisory** |
| ☐ | **Other** | ☐ | **None** |

| | |
|---|---|
| Describe each applicable format. | Forms that collect personal data will contain a Privacy Act Statement, as required by 5 USC 552a(e)(3), and under Executive Order or EO 9397 and 13478 (SSN), as the authority to collect the social Security number and in accordance with guidelines established in AFI 33-332, Privacy Act Program, Chapters 3 and 7, and 12, allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the Air Force Privacy Act Office during the comment period (if applicable), during data collection, or at any time after the program is launched. If no objections are received, consent is presumed. |

**NOTE:**

**Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.**

**A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.**

## SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

**a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.**

**(1) What PII will be collected?** Indicate all individual PII or PII groupings that apply below.

| | | |
|---|---|---|
| ☒ Name | ☐ Other Names Used | ☒ Social Security Number (SSN) |
| ☒ Truncated SSN | ☐ Driver's License | ☐ Other ID Number |
| ☐ Citizenship | ☐ Legal Status | ☒ Gender |
| ☒ Race/Ethnicity | ☒ Birth Date | ☒ Place of Birth |
| ☒ Personal Cell Telephone Number | ☒ Home Telephone Number | ☒ Personal Email Address |
| ☒ Mailing/Home Address | ☒ Religious Preference | ☐ Security Clearance |
| ☐ Mother's Maiden Name | ☐ Mother's Middle Name | ☐ Spouse Information |
| ☐ Marital Status | ☐ Biometrics | ☐ Child Information |
| ☒ Financial Information | ☒ Medical Information | ☒ Disability Information |
| ☐ Law Enforcement Information | ☒ Employment Information | ☐ Military Records |
| ☐ Emergency Contact | ☐ Education Information | ☒ Other |

| | |
|---|---|
| If "Other," specify or explain any PII grouping selected. | Financial information relative to rank only; Most PII items are collected when relevant to the basis/nature of the complaint. |

**(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?**

Information is collected from the field(s) being updated by the personnelist as requiring by policy, procedure or public law either in-person or through personnel forms updated at a Military Personnel Flight (MPF) or in some cases by the individual, or authorized user. The information is behind a secure layer, to ensure the information is not lost or given to people that are not authorized.

**(3) How will the information be collected?** Indicate all that apply.

| | | | |
|---|---|---|---|
| ☒ | **Paper Form** | ☒ | **Face-to-Face Contact** |
| ☒ | **Telephone Interview** | ☒ | **Fax** |
| ☒ | **Email** | ☐ | **Web Site** |
| ☒ | **Information Sharing - System to System** | | |
| ☐ | **Other** | | |

If "Other," describe here.

**(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?**

PII is collected to identify individuals involved in the complaint process, such as complainant, witnesses, alleged offender. Some PII is required to complete case processing and is collected from individuals for that purpose, such as date of birth, age, race, etc.

**(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?**

Administrative use: data must be collected to confirm identification and to complete case information requirements. Additionally, the data is used for producing reports IAW EEOC legal guidelines.

**b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation?** (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

**If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.**

**c. Who has or will have access to PII in this DoD information system or electronic collection?** Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☐ **Contractors**

☐ **Other**

If "Other," specify here.

**d. How will the PII be secured?**

**(1) Physical controls.** Indicate all that apply.

| | | | |
|---|---|---|---|
| ☐ | **Security Guards** | ☒ | **Cipher Locks** |
| ☒ | **Identification Badges** | ☐ | **Combination Locks** |
| ☒ | **Key Cards** | ☒ | **Closed Circuit TV (CCTV)** |
| ☐ | **Safes** | ☐ | **Other** |

Currently AFEON decision makers have not determined where the system will physically reside, the two options are either a DISA DECC or HQ AFPC, however the physical controls requirements will be met regardless of either facility.

**(2) Technical Controls.** Indicate all that apply.

| | | | |
|---|---|---|---|
| ☒ | **User Identification** | ☐ | **Biometrics** |
| ☒ | **Password** | ☒ | **Firewall** |
| ☒ | **Intrusion Detection System (IDS)** | ☐ | **Virtual Private Network (VPN)** |
| ☒ | **Encryption** | ☒ | **DoD Public Key Infrastructure Certificates** |
| ☐ | **External Certificate Authority (CA) Certificate** | ☒ | **Common Access Card (CAC)** |

☐ **Other**

Currently AFEON decision makers have not determined the security front-end for the system, the two options are AFPC Secure or the A1 Portal which has not been finalized, however either front-end will meet all security requirements in 8500.2.

Access to the AFEON application is Role Based; only personnel with assigned roles can access personnel data within the application.

The PIA is based on proper implementation, validation, and verification of the baseline information

assurance (IA) controls for CONFIDENTIALITY, in accordance with Department of Defense Instruction (DoDI) 8500.2, “Information Assurance Implementation.”

**(3) Administrative Controls.** Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

If "Other," specify here.

**e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?**

☒ **Yes. Indicate the certification and accreditation status:**

| | | | |
|---|---|---|---|
| ☐ | **Authorization to Operate (ATO)** | **Date Granted:** | |
| ☐ | **Interim Authorization to Operate (IATO)** | **Date Granted:** | |
| ☐ | **Denial of Authorization to Operate (DATO)** | **Date Granted:** | |
| ☒ | **Interim Authorization to Test (IATT)** | **Date Granted:** | Will submit for UIAR upon acquiring system HW/SW |

☐ **No, this DoD information system does not require certification and accreditation.**

**f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?**

Individuals' privacy will be secured at all levels of the information life cycle. The collection of information derives from whichever medium the EO complaint was submitted to the EO office at which point the EO officer inputs the complaint into AFEON. While in use the individuals' data will reside on the AFEON database server in a secure state meaning it will have been run against a DISA STIG, Gold Disk, and had a vulnerability scan ran. The EO complaint will reside internal to AFEON in a secure state for as long as the applicable law states for either active military or DoD civilians. In the event a hard drive on a server needs to be sanitized, it will go through the appropriate DoD degaussing procedures in an approved degausser.

**g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?**

Information is used for official use only. Role based access restricts use by unauthorized users of the system. Measures include CAC enabled, firewalls, SSL (https), intrusion detection, and port security.

**h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?**

Unless the system is hacked, vulnerability of privacy information is minimal. If the system is compromised the following could be at risk: General customer demographics; Social Security Numbers and any information in the EO Complaint. The risks of compromise to this information is minor since the records will the stored in a restricted area of HQ AFPC or a DISA DECC and only administrators and individuals with need-to-know will have access.